

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2003年 3月20日

出 願 番 号

Application Number:

特願2003-076788

[ST.10/C]:

[JP 2003-076788]

出 願 人

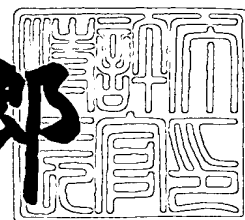
Applicant(s):

株式会社日立製作所

2003年 6月10日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3044977

【書類名】 特許願

【整理番号】 D03000391A

【あて先】 特許庁長官殿

【国際特許分類】 G11B 7/00

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
製作所デジタルメディア開発本部内

【氏名】 石飛 竜哉

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
製作所デジタルメディア開発本部内

【氏名】 小野 裕明

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
製作所デジタルメディア事業部内

【氏名】 大矢 淳

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 ディスク管理情報の認証方法およびディスク装置

【特許請求の範囲】

【請求項 1】

ディスクに記録された記録データの管理情報が有効であるか否かの判定のための認証情報を有するディスクの管理情報の認証方法であって、
認証情報と、管理情報とを記録データと同じディスク上に記録し、
認証情報が有効な認証情報の場合は、管理情報を有効であるとし、
認証情報が無効な認証情報の場合は、管理情報を無効であるとする
ことを特徴とするディスク管理情報の認証方法。

【請求項 2】

ディスクに記録された記録データの管理情報の認証方法であって、
記録データと同じディスクに記録された管理情報が有効である否かの判定に、
管理情報が有効であることを示す管理情報と同じディスクに記録された認証情報
と、認証情報を無効化する管理情報と同じディスクに記録された認証無効化情報
を用い、
認証情報が認証無効化情報によって無効化されていない場合は、管理情報を有効
であるとし、
認証情報が認証無効化情報によって無効化されている場合には、管理情報を無効
であるとする
ことを特徴とするディスク管理情報の認証方法。

【請求項 3】

請求項 2 記載のディスク管理情報の認証方法であって、
認証情報は、ディスク装置の電源が切断される、あるいはディスク装置からディ
スクが排出される等のとき行われるディスク装置の停止処理において、ディスク
に記録された管理情報が有効な場合に管理情報と同じディスクに記録され、
認証無効化情報は、ディスク装置の電源が投入される、あるいはディスクが交換
される、あるいはディスクが再挿入される等のときディスク装置が起動したのち
、ディスク装置における初めての記録処理のとき管理情報と同じディスクに記録

されることを特徴とするディスク管理情報の認証方法。

【請求項 4】

請求項 2 記載のディスク管理情報の認証方法であって、
認証情報と認証無効化情報とを同じ記録領域に、かつ、時系列的に記録すること
を特徴とし、
同領域を順次走査することによって、認証情報を無効化する認証無効化情報の有
無を確認することが可能なことを特徴とするディスク管理情報の認証方法。

【請求項 5】

請求項 2 記載のディスク管理情報の認証方法であって、
認証情報をディスク上の試し書き領域に記録することを特徴とし、さらに、試し
書き領域に通常に記録される試し書き用パターンを認証無効化情報として利用す
ることを特徴とするディスク管理情報の認証方法。

【請求項 6】

ディスクに記録された記録データの管理情報と、管理情報が有効であるか否か
を判定する認証情報と、認証情報を無効化する認証無効化情報とを時系列的に、
記録データと同じディスク上に記録する記録手段を有し、
ディスク装置における電源投入後あるいはディスク挿入後の起動処理において、
認証情報が認証無効化情報によって無効化されていない場合は、管理情報を有効
であると判断し、認証情報が認証無効化情報によって無効化されている場合は、
管理情報を無効であると判断する判断手段を有することを特徴とするディスク装
置。

【請求項 7】

請求項 6 記載のディスク装置であって、
ディスク装置の電源が切断される、あるいはディスク装置からディスクが排出さ
れる等のときのディスク装置の停止処理において、ディスクに記録された管理情
報が有効と確認された場合に、認証情報を記録し、
ディスク装置の電源が投入される、あるいは、ディスクが交換される、あるいは
ディスクが再挿入される等のときのディスク装置の起動処理あるいは記録処理に
おいて認証無効化情報を記録することを特徴とするディスク装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ディスク装置における特にディスクの管理情報の有効性の認証方法に関するものである。

【 0 0 0 2 】

【従来の技術】

一連のデータをシーケンシャルに追記して行くディスク、例えばDVD-Rのようなディスクには、データ領域における記録の進捗状況等を含む管理情報を記録するための管理領域が設けられている。ディスク装置は、装置の電源が投入された、あるいは、装置にディスクが挿入された等を契機とした起動処理において、ディスク上の管理領域から最新の管理情報を読み出す。読み出した管理情報からデータ領域における記録進捗を知ることができるため、ディスク装置はそれによってデータ領域における追記開始位置を特定することができる。ただし、記録進捗情報が常にデータ領域の記録状態と合致するとは限らないため、従来はデータ領域を走査して管理情報から得られる記録進捗情報が正しいか否かを確認する必要があった。その具体例を、図4～図7を用いて未記録状態のDVD-Rディスクにデータを記録する際の過程も含めて説明する。

【 0 0 0 3 】

図4は、DVD-Rディスク上の三つの領域を模したものである。また、図4は、各領域は未記録状態であることを表している。図4において401はディスク装置が適正な記録パワーを求めるために使用する試し書き領域PCA (Power Calibration Area) である。402は管理情報であるRMD (Recording Management Data) を記録するための領域RMA (Recording Management Area) である。403はデータを記録するためのデータ領域DA (Data Area) である。各領域は全て左側がディスクの内周側に相当し、右側がディスク外周に相当する。実際のDVD-Rでは三つの領域のうち、PCAが最も内周寄りにあり、次いでRMA、その後DAと続く。また、各領域の大きさを変えて記してあるのは、各領域の記録容量を表したがためであり、データ領域であるDA 403はディスク上の殆どの領域を占めることを表している

【 0 0 0 4 】

図 4 に示した未記録状態の DVD-R ディスクがディスク装置に挿入された後、ホスト装置からディスク装置に対して記録モードの指定があるとディスクは図 5 に示す状態に遷移するがその手順は次の通りである。

【 0 0 0 5 】

ディスク装置はホスト装置から記録モードを指定されると、適正な記録パワーを求めるための試し書きを PCA 401 において行う。図 5 の PCA 401 内の 501 はその試し書きの際に記録されたテストパターンを表す。ディスク上の各領域は、内周から外周に向かって順次記録を行うことが規格で定められているが、試し書き領域に限っては外周から内周に向かって順次記録することが定められているため、テストパターン 501 の記録位置は PCA 401 の最外周側に記録される。

【 0 0 0 6 】

ディスク装置は試し書きを終えると、RMA 402 にホスト装置から指定のあったディスクの記録モードを含む管理情報 RMD を記録するが、502 がその RMD を表す。図 5 には明示していないが記録モードは追記が可能なインクリメンタル記録モードが指定されたものとし、図 5 に示す状態に遷移することによって初めてディスク上のデータ領域への記録が可能になる。

【 0 0 0 7 】

ディスクが図 5 の状態にあるときに、ディスク装置がホスト装置よりデータの記録指示され、データを記録した後のディスクの状態が図 6 である。図 6 の 601 は記録されたデータである。また、602 はデータ 601 の記録が終了した際に、データ領域における記録の進捗を管理するためにディスク装置の判断によって新たに記録された RMD である。RMD はデータを記録する度に記録されるものではなく、通常は、記録したデータの総データ量が規定の量を超えた場合にディスク装置の判断に基づいて記録される。図 6 は、データ 601 のデータ量が新たな RMD を記録するための基準を超えたケースであることを表している。

【 0 0 0 8 】

ディスクが図 6 の状態にあるときに、ディスク装置がホスト装置より二つのデ

ータの記録を順次指示され、二つのデータを順次記録した後のディスクの状態が図 7 である。図 7 は、ディスク装置がホスト装置からデータ 701、データ 702 の順に記録を指示され、それらを順次記録したことを表している。図 7 では、記録したデータ 701、データ 702 の総データ量は新たな RMD を記録する基準に満たないことから新たな RMD は記録されず、図 6 の状態と同様に 602 が最新 RMD となっていることを表している。従って、図 7 の状態は、最新 RMD から得られるデータ領域における記録進捗情報と実際の記録領域の記録状態が合致しないケースを表している。

【 0 0 0 9 】

ここで、図 7 に示す状態のディスクがディスク装置より排出された後、再び、ディスク装置に図 7 に示す状態でディスクが挿入された場合に、従来、ディスク装置が行っていた処理について説明する。

【 0 0 1 0 】

ディスク装置はディスクが挿入されると RMA 402 を内周側より走査し、既記録の領域と未記録の領域との境界を検出する。そして、検出した境界に隣接する RMD 602 を最新の RMD として認識する。ただし、ディスク装置は RMD 602 が RMA 402 内で最も新しいことは分かっても、RMD 602 から得られる記録進捗情報がデータ領域における実際の記録状態と合致しているか否かは分からない。（図 7 に示した例では実際に合致していないがそのことをディスク装置は知る術がない。）そこで、ディスク装置は RMD 602 より得られる記録進捗情報をもとにデータ領域を走査し、データ 702 の最後尾で既記録状態から未記録状態となる位置を検出し、追記を開始すべき位置がデータ 702 の最後尾の次からであると特定する。

【 0 0 1 1 】

続いて、図 6 に示す状態のディスクがディスク装置より排出された後、再び、ディスク装置に図 6 に示す状態でディスクが挿入された場合のディスク装置の処理について説明する。ディスク装置はディスクが挿入されると RMA 402 を内周側より走査し、既記録の領域と未記録の領域との境界を検出する。そして、検出した境界に隣接する RMD 602 を最新の RMD として認識する。ただし、ディスク装置は RMD 602 が RMA 402 内で最も新しいことは分かるが、ディスク装置は RMD 602 から得

られる記録進捗情報がデータ領域における実際の記録状態と合致しているか否かは分からない。（図 6 に示した例では実際には合致しているので本来であればデータ領域を走査する必要はないが、そのことをディスク装置は知る術がない。）そこで、図 7 のケースで説明したのと同様に、RMD 602 より得られる記録進捗情報をもとにデータ領域を走査し、データ 601 の最後尾で既記録状態から未記録状態となる位置を検出し、追記を開始すべき位置がデータ 601 の最後尾の次からであると特定する。

【 0 0 1 2 】

従来このような問題に対応するために、ディスク装置の上位装置内に不揮発性メモリを設け、ディスクに記録されるべき管理情報と同一の内容をこの不揮発性メモリに保持しておくという方法が考案されている。（特許文献 1 参照）

この従来方法は、上位装置がディスク装置に対して記録指示する前にディスク装置にディスク上の最新の管理情報を報告させ、ディスク装置から報告され管理情報と不揮発性メモリ内の管理情報とが不一致となった場合に、不揮発性メモリ内の管理情報をディスクに記録するようディスク装置に指示するというものである。また、最新の管理情報が常に不揮発性メモリに格納されているので、記録を行う前にデータ領域の走査を行って管理情報の有効性をチェックする必要がないというものである。

【 0 0 1 3 】

ただ、この従来方法は、上位装置に設けられた不揮発性メモリに、記録を行おうとするディスクに付随する管理情報が格納されていなければ成立せず、その場合は、管理情報が有効である有効でないにかかわらずデータ領域の走査が必要であった。また、本来はディスク装置が管理すべき情報をその上位装置が管理するという点で大掛かりであった。さらには、複数枚のディスクについて管理情報を保持する場合は、不揮発メモリにそれ相応の記憶領域が必要であるためコストの点で問題があり、また、ディスクとそれに対応する不揮発メモリ内の管理情報との対応付けを行う必要があるため上位装置とディスク装置との間の手続きが煩雑であった。

【 0 0 1 4 】

以上、説明したように従来はディスクの管理情報の有効性を確認する方法が十分でなかったために、ディスク装置においてディスク上のデータ領域の走査を行わなければならなかった。また、データ領域の走査を回避するために上位装置による管理情報の管理が考案されていたが、ディスク装置単独で管理情報を管理することができないという点で十分ではなかった。

【 0 0 1 5 】

【特許文献 1】

特開 2 0 0 2 - 3 1 2 9 4 0 号公報（第 6 - 7 頁、段落番号 0 0 5 8、第 5 図）

【 0 0 1 6 】

【発明が解決しようとする課題】

以上、説明した通り、従来は、管理情報である RMD から得られる記録進捗情報と、実際のデータ領域の記録状態が合致しているか否かを知る術がなかったので、合致している、合致していないにかかわらずデータ領域の走査が必要であった。そのため、ディスク装置は起動処理に時間を要し、ディスク挿入後あるいは電源投入後、直ちに記録可能な状態に移行することが出来ないという問題を引き起こしていた。

このことは、電源投入後あるいはディスク挿入後、短時間のうちに記録可能な状態になることが要求されるシステムにおいて特に問題となっていた。例えば、ディスク装置を搭載したビデオカメラがそれに該当する。ビデオカメラでは、ユーザーが撮影を行いたいと思い電源を投入した場合に直ちに撮影が可能な状態に移移することが要求される。ビデオカメラにおいて、搭載されたディスク装置がディスクの記録開始可能な位置を確定するために時間を要してしまうと、ビデオカメラは撮影可能な状態に入ることが出来ず、ユーザーが撮影した場面を取り逃すことにつながってしまう。また、データ領域を走査した結果、管理情報とデータ領域の記録状態が不一致であった場合はそれらの整合性をとるための処理が必要な旨をユーザーに伝える等の対応をとる必要があるが、電源投入後しばらく時間を置いてからそのようなことを伝えられると、ユーザーはその応答性に違和感を覚えることになる。

【 0 0 1 7 】

本発明は、ディスク装置の電源投入、あるいは、ディスク挿入などのときのディスク装置における起動処理において、ディスク上の管理領域に記録された最新の記録進捗情報がデータ領域の記録状態と合致する有効な情報であるか否かを短時間に判定できるようにし、その結果としてディスク装置の応答性を高めることを課題とする。

【 0 0 1 8 】

【課題を解決するための手段】

本発明は課題を解決するために、ディスクに対し新たに二つの情報を記録する。

【 0 0 1 9 】

一つ目は、管理領域に記録される記録進捗情報がデータ領域の最新の記録状態を合致することを認証する認証情報である。この認証情報はディスク装置の電源切断あるいはディスク排出などのときのディスク装置の停止処理において、管理情報と同じディスク上に記録される。

【 0 0 2 0 】

二つ目は、認証情報を無効化する役割を果たす認証無効化情報である。この認証無効化情報は、ディスク装置の電源投入あるいはディスク装置へのディスク挿入などのときディスク装置が起動した後、ディスク装置における最初の記録処理において認証情報と同じディスク上に記録される。

【 0 0 2 1 】

ディスク装置の電源投入あるいはディスク装置へのディスク挿入などのときのディスク装置の起動処理中において本発明が提供するディスク上の認証情報の有効性を確認することによって、短時間のうちに同ディスク上の管理情報の有効性を確認することができる。

【 0 0 2 2 】

本発明が提供する技術によってディスク装置では、電源投入、あるいは、ディスク挿入などのときの起動処理において、ディスクに記録された管理情報の有効性を短時間に確認することができるようになる。これによって、ディスク装置は

記録可能な状態へと遷移することが可能か否かを早期に判断することができるようになる。本発明が提供する技術は、ビデオカメラのようにユーザーがビデオカメラの電源投入後あるいは記録媒体挿入後直ちに撮影可能な状態に遷移することを求められるシステムにおいて、ディスク装置を記録手段として採用する場合に有用である。

【 0 0 2 3 】

【発明の実施の形態】

まず、本発明の要点を、図 1 ～図 3 を用いて以下説明する。

【 0 0 2 4 】

図 1 は、本発明の要点であるディスクに記録された管理情報の有効性を確認する手順を示すものである。図 1 に示す手順は、ディスク装置における電源投入あるいはディスク挿入等のときの起動処理において実施することで効果を発揮するものである。

【 0 0 2 5 】

その効果とは、管理情報の有効性を確認するために従来行われていたディスク上のデータ領域の走査、これを行うことなく管理情報の有効性を確認することができるというものである。管理情報の有効性とは、管理情報から得られ、ディスク上の各データ領域についてどこまで記録を行ったかということを表す記録進捗情報が、データ領域の実際の記録状態と合致する有効な情報であるか否かということである。従来は管理情報の有効性を確認する為に、管理情報に含まれる記録進捗情報に基づいてデータ領域を走査し、記録進捗情報とデータ領域の記録状態が合致しているか否かを確認するという処理を行っていた。この処理は通常、ディスク装置における電源投入あるいはディスク挿入等のときの起動処理中において行われるが、この処理に時間を要するため起動処理時間が長くなり、ディスク装置の応答性を低下させていた。本発明は従来のこのような問題を解消するものであるが、その鍵となるのが管理情報の有効性を認証する認証情報であり、この認証情報は本発明によって提供されるものである。

【 0 0 2 6 】

認証情報は、図 1 に示すように 102 において管理情報の存在が確認されると、1

03において認証情報がディスクより取得される。そして、取得された認証情報が104において有効と判定されると、105において管理情報の有効性が認証情報によって確認される。認証情報によってデータ領域を走査することなく管理情報の有効性を確認することができるため、管理情報が有効と判定された場合には起動処理時間の短縮を図ることができる。管理情報が有効と判定されなかった場合においては図1に示す106に示すデータ領域の走査を行うことになるが、走査を行う前に既に管理情報が無効であること、あるいは無効の可能性があることが分かるため、走査開始前にディスク装置のホスト装置あるいはディスク装置のユーザーに対して管理情報が無効または無効の可能性があるがためにその対応が必要である等の通報を行うことが可能になる。従って、管理情報が無効あるいは無効な可能性がある場合においてもディスク装置のホスト装置あるいはユーザーに対しての応答性を高めることができる。

【 0 0 2 7 】

なお、認証情報のディスクへの記録手順については後に図2を用いて説明する。また、認証情報が如何にして有効と確認することができるかは後に図3を用いて説明する。

【 0 0 2 8 】

図1の103において認証情報が取得されることを説明したが、その認証情報がディスクに記録される手順を示すものが図2である。図2に示す手順は、ディスク装置における電源切断あるいはディスク排出等のときの停止処理中において実施されるべきものである。ディスク装置の停止処理中に図2に示す手順が実施されると、まず、202においてデータ領域の記録状態と合致する記録進捗情報を含む最新の管理情報が既にディスクに記録されているか否かが確認される。ここで、既に記録済であると確認されると、204において認証情報が管理情報と同じディスク上に記録されて手順を終了する。202においてデータ領域の記録状態と合致する記録進捗情報を含む管理情報が未だディスクに記録されていないことか確認されると、203においてデータ領域の記録状態と合致する記録進捗情報を含む管理情報が記録され、この後、204において認証情報が管理情報と同じディスク上に記録されて手順を終了する。図2に示す手順をディスク装置の停止処理中に

おいて行うことによって、データ領域の記録状態と合致する記録進捗情報を含む管理情報がディスク上に記録され、かつ、その管理情報が有効であることを証明するための認証情報も管理情報と同じディスク上に記録される。

【 0 0 2 9 】

図 1 の 104 において認証情報の有効性が確認されることを説明したが、その有効性を否定するための手順を示すものが図 3 である。これはディスク装置において記録処理を行う場合に踏まれる手順であり、図 3 に示すように 302 においてディスク装置における起動後、初めての記録処理か否かが確認され、初めての記録処理の場合に限って 303 において認証情報が無効であることを表す情報がディスク上に記録され、認証情報の無効化が達成される。図 3 に示す手順はディスク上に認証情報が記録されている記録されていないかわらず有効であり、図 3 に示す手順がディスク上に認証情報が記録されている状態で行われた場合でも、ディスク上に未だ認証情報が記録されていない状態で行われた場合でも、認証情報が無効であるとの状態を作り出す。

【 0 0 3 0 】

以上、図 1 ～図 3 を用いて説明した本発明による処理を、DVD-R を記録媒体とするディスク装置への適用を例にとり、図 8 および図 9 を用いて以下説明する。本例では、本発明で言うところの認証情報を管理情報である最新 RMD のコピーとし、本発明で言うところの認証無効化情報を試し書き領域である RMA に記録されるテストパターンとする。

【 0 0 3 1 】

まず、図 8 を用いて図 2 に示す認証情報記録処理について説明する。図 8 は、ディスク装置に挿入されているディスクが図 6 に示す状態にある時に、ディスク装置がディスクの排出指示を受けて停止処理を行い、停止処理の一環として図 2 を用いて説明した本発明による認証情報記録処理を行った後のディスクの状態を示している。認証情報記録処理において図 6 に示す状態のディスクは、最新の RMD 602 から得られる記録進捗情報とデータ領域における実際の記録状態が合致していることから、RMD 602 が真に最新の管理情報であると判断され、それを証明するための認証情報 801 が試し書き領域である PCA 401 に既に記録されてい

るテストパターン501に追記される形で記録される。(RMD 602がデータ領域の記録状態と合致していない場合は、データ領域の記録状態を反映したRMDが新たに記録され、この後、認証情報が記録される。)なお、認証情報の内容は先に説明したが、最新RMDのコピーであり、図8では、RMD602と同一の内容となる。また、認証情報は必ずしも試し書き領域であるPCA 401に記録する必要はないが、本例では、認証情報を無効化する認証無効化情報をPCA 401に記録されるテストパターンとし、認証情報と認証無効化情報を同じ領域に記録したほうが認証情報の有効性の有効性確認手順が簡便になることから、PCAを認証情報の格納領域として採用した。

【0032】

次に、図8を用いて図1に示す管理情報認証処理について説明する。図8に示す状態のディスクがディスク装置に挿入されると、ディスク装置は管理領域RMA 402を走査し、RMD 602が最新のRMDであると認識する。そして、図1に示す本発明による管理情報認証処理が行われる。管理情報認証処理においては、管理情報が存在することから認証情報取得、さらには認証情報の有効性の確認が行われる。認証情報の有効性は、試し書き領域であるPCA 401を内周側から外周側に向かって走査し、記録状態が未記録から既記録に変わる境界の直後に記録された情報を認証情報として取得し、取得した情報が認証情報のデータ構造である場合には認証情報が有効であると判断され、認証無効化情報として流用したテストパターンのデータ構造である場合には認証情報が無効と判断される。

【0033】

図8の場合、PCAの走査によって検出される未記録部と既記録部との境界位置に存在する認証データ801は、テストパターンではなく、RMD 602のコピーであるため、そのことによって801は認証データとして有効であると確認される。そして、有効と確認された認証データ801と最新の管理情報であるRMD602の全内容または一部内容が比較される。図8では両者は一致するので、RMD 602から得られるデータ領域における記録進捗情報が、データ領域における実際の記録状態と合致することが証明される。従って、ディスク装置はデータ領域の走査を行うことなく、データ領域における追記開始位置を特定することができる。ま

た、これによって、ディスク装置は起動処理を短時間に終えることが可能となる。

【 0 0 3 4 】

最後に、図 3 を用いて説明した認証情報無効化処理について図 9 を用いて説明する。図 9 は、図 8 に示す状態のディスクがディスク装置挿入され、ディスク装置が起動処理を終了した後、ホスト装置より記録指示があり、その指示従ってデータを記録した結果のディスク状態を示すものである。ディスク装置は、ホスト装置より記録指示を受けると、最適な記録パワーを求めるために PCA 401 において試し書きを行い、テストパターン 901 が認証情報 801 に追記される形で記録される。また、テストパターン 901 は認証情報 801 を無効化する認証無効化情報としての役割を果たす。図 3 を用いて説明した認証情報無効化処理では、記録指示を受けた時点で、その記録指示が起動後初めてのものであった場合に認証無効化情報を記録すると説明したが、起動後、初めての記録においては、通常のディスク装置では必ず記録パワーを調整する必要があることから、テストパターンを認証無効化データとして流用する例を示した。この後、データ 902 が記録され、ディスクは図 9 に示す状態となる。

【 0 0 3 5 】

仮に、ディスクが図 9 に示す状態でディスク装置において起動処理が行われたとする。（このケースは、例えば、ディスクが図 9 の状態で不慮の電源切断によってディスク装置が停止され、再度、ディスク装置の電源が投入された場合などに起こり得る。）ディスク装置は起動処理の一環として、RMA 402 を走査することによって RMD 602 を最新の RMD と認識した後、PCA 401 を走査し、未記録部と既記録部の境界を検出し、境界に接するテストパターン 901 を取得する。取得された 901 はテストパターンであり RMD のデータ構造をしていないため、認証情報は無効と確認される。従って、この時点で、RMD 602 から得られるデータ領域の記録進捗情報はデータ領域の実際の記録状態と一致しないと判断され、データ領域の走査が行われる。データ領域の走査が必要であるという点は従来と同様であるが、本発明ではデータ領域の走査を行う前に管理情報である RMD が無効である、あるいは無効である可能性があることを判断することことがで

きる。そのため、この時点でデータ領域の走査が必要であり、処理に時間を要する可能性がある等の通報をホスト装置あるいはユーザーに対して行うことができる。従って、データ領域の走査を行う必要性をホスト装置あるいはユーザーに知らしめた上でデータ領域の走査を実際に行うことができることからディスク装置の応答性を向上させることができる。

【 0 0 3 6 】

以上、本発明の実施例を示したが、本発明は、従来のディスク装置において本発明が提供する処理手順を採用することのみで実現される。ディスク装置における処理手順は、通常、マイコン上で動作するソフトウェアによって実行される。また、ディスクに情報を記録する、あるいは、ディスクから情報を読み取り、読み取った内容を見る、比較する等の基本機能は通常のディスク装置には全て備わっている。従って、本発明はディスク装置に対しハードウェア部品を追加する必要はなく、ソフトウェアを変更するだけでよく実現される。

【 0 0 3 7 】

【発明の効果】

本発明によりディスク装置は、装置の電源投入あるいはディスク挿入などのときの起動処理において、ディスク上の管理情報から得られる記録進捗情報がデータ領域における実際の記録状態と合致しているか否かを、データ領域の走査を行うことなく確認することが可能になる。これによって、管理情報が有効であると判定した場合には、データ領域の走査を行う必要がないため、起動処理を短時間のうちに終えることができ、結果としてディスク装置の応答性を高めることが可能になる。また、管理情報が無効であると判定した場合には、データ領域の走査を行うことになるが、データ領域の走査を行う前にホスト装置あるいはユーザーに対して時間を要するデータ領域の走査を行う必要性がある等を通報する機会を得ることができるため、結果としてディスク装置の応答性を高めることができる。

。

【図面の簡単な説明】

【図 1】

本発明による管理情報認証処理の手順を示す図。

【図 2】

本発明による認証情報記録処理の手順を示す図。

【図 3】

本発明による認証情報無効化処理の手順を示す図。

【図 4】

未記録状態の DVD-R ディスクの状態を表す模式図。

【図 5】

図 4 に示すディスクについて、記録モードが決定された後のディスク状態を示す模式図。

【図 6】

図 5 に示すディスクに対してデータが記録され、新たな管理情報が記録されたディスク状態を示す模式図。

【図 7】

図 6 に示すディスクに対し、新たなデータが記録されたディスク状態を示す模式図。

【図 8】

図 6 に示すディスクに対し、本発明が提供する認証情報が記録された後、データが記録および管理情報が記録されたディスク状態を示す模式図。

【図 9】

図 7 に示すディスクに対し、本発明が提供する認証無効化情報が記録された後、データが追記されたディスク状態を示す模式図。

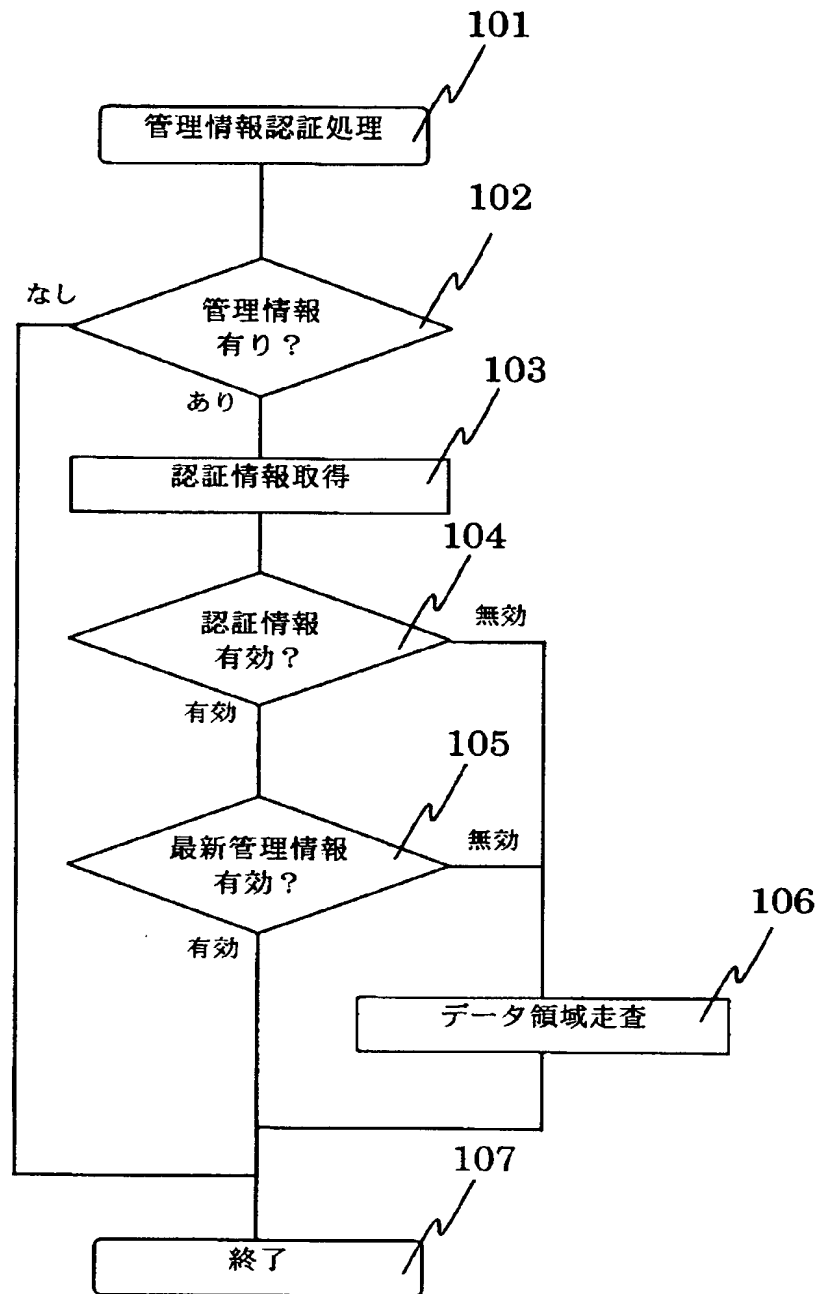
【符号の説明】

- 1 0 1 . . . 管理情報認証処理、
- 2 0 1 . . . 認証情報記録処理、
- 3 0 1 . . . 認証情報無効化処理。

【書類名】 図面

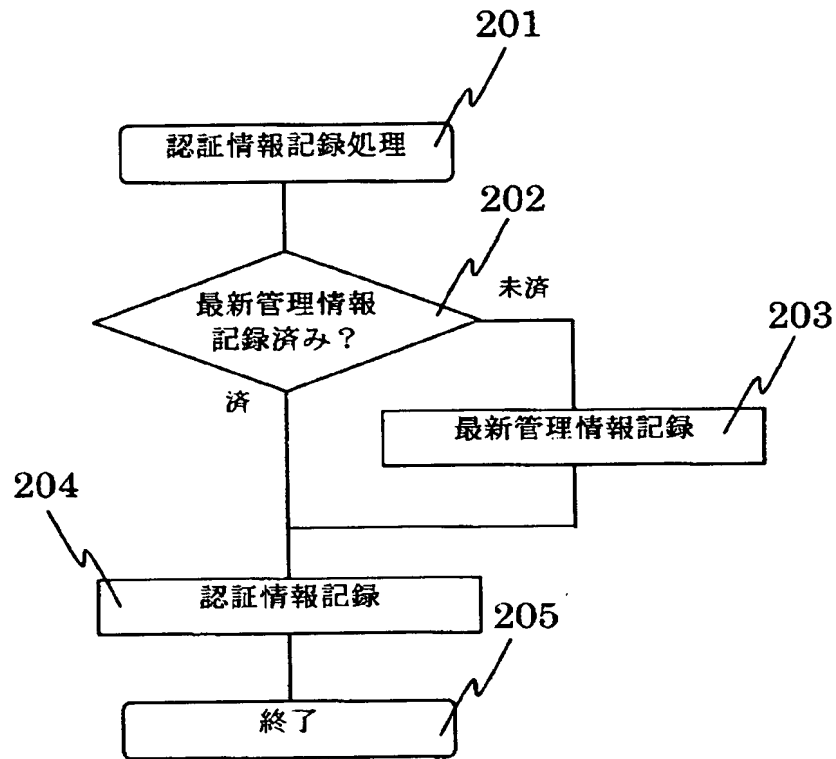
【図 1】

図 1



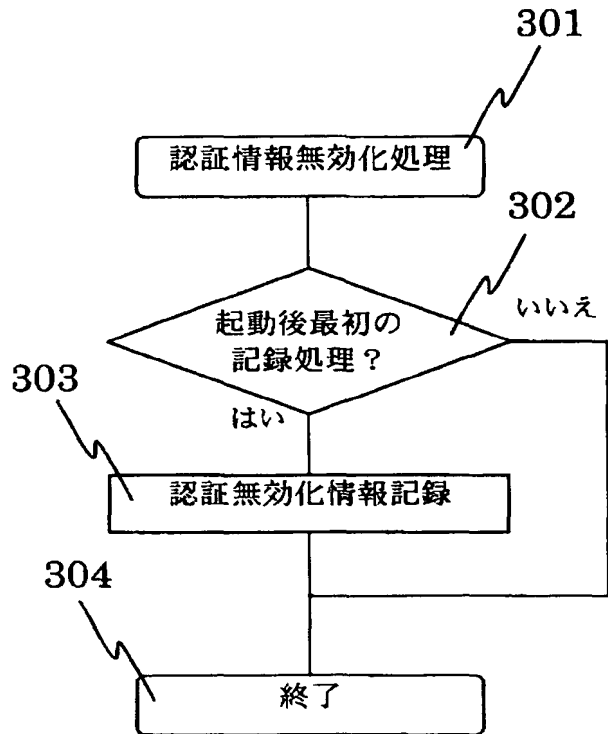
【図 2】

図 2



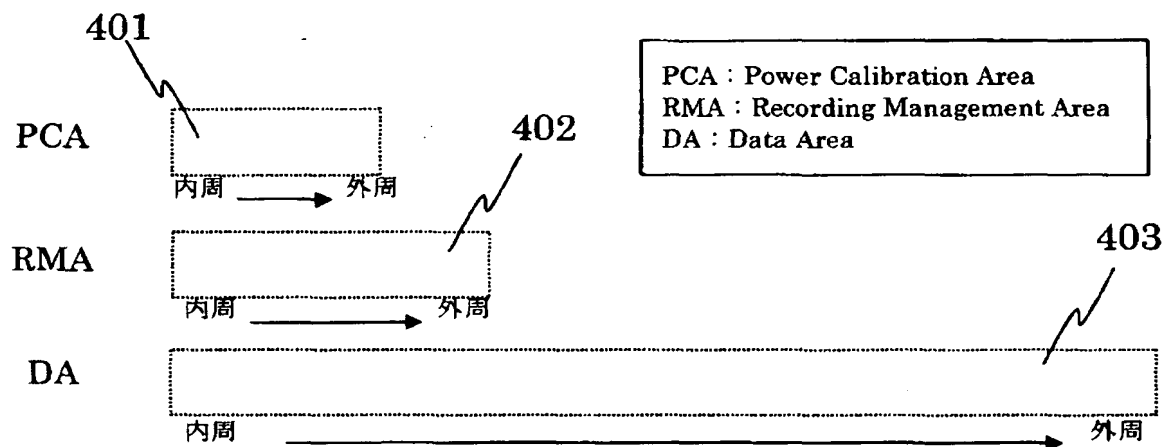
【図 3】

図 3



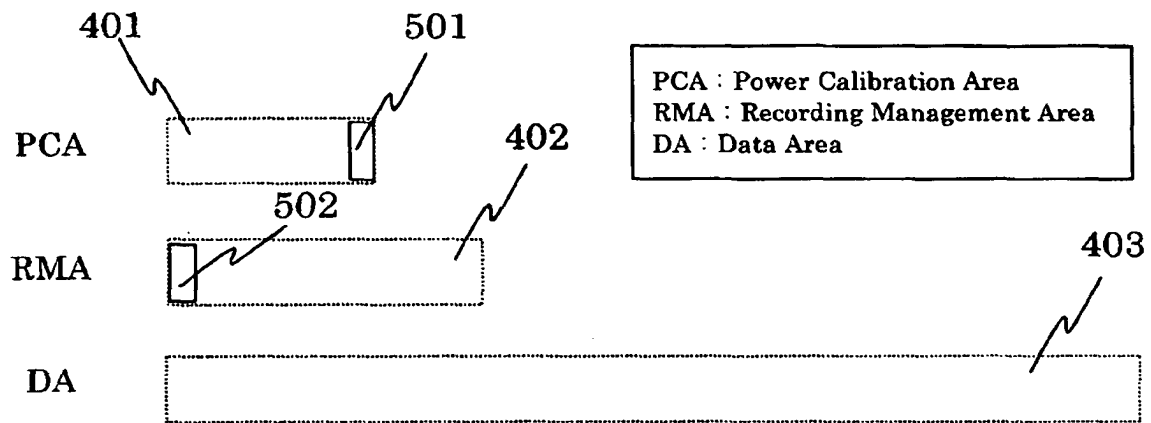
【図 4】

図 4



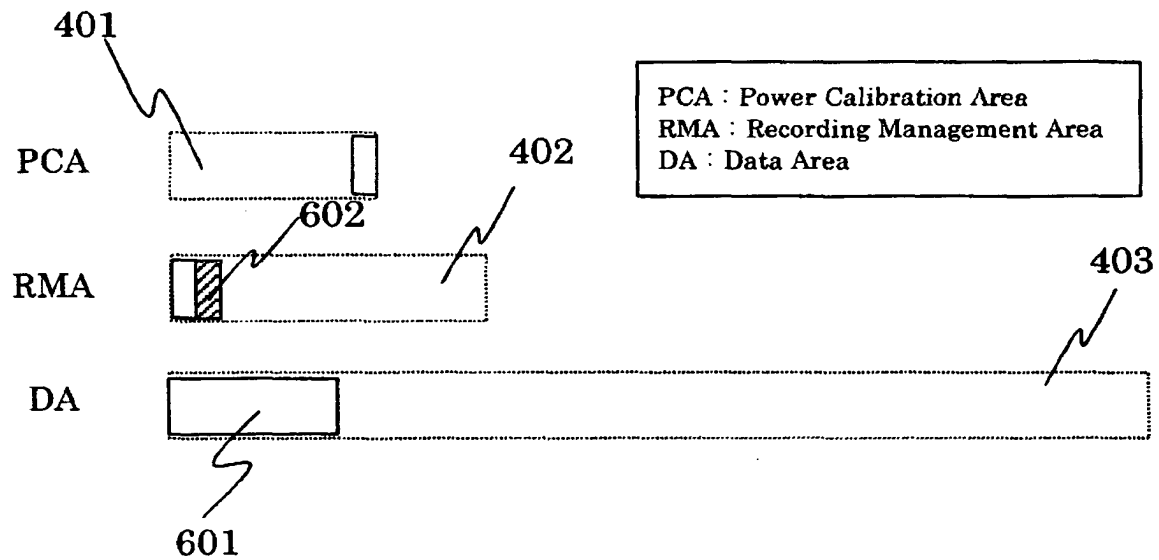
【図 5】

図 5



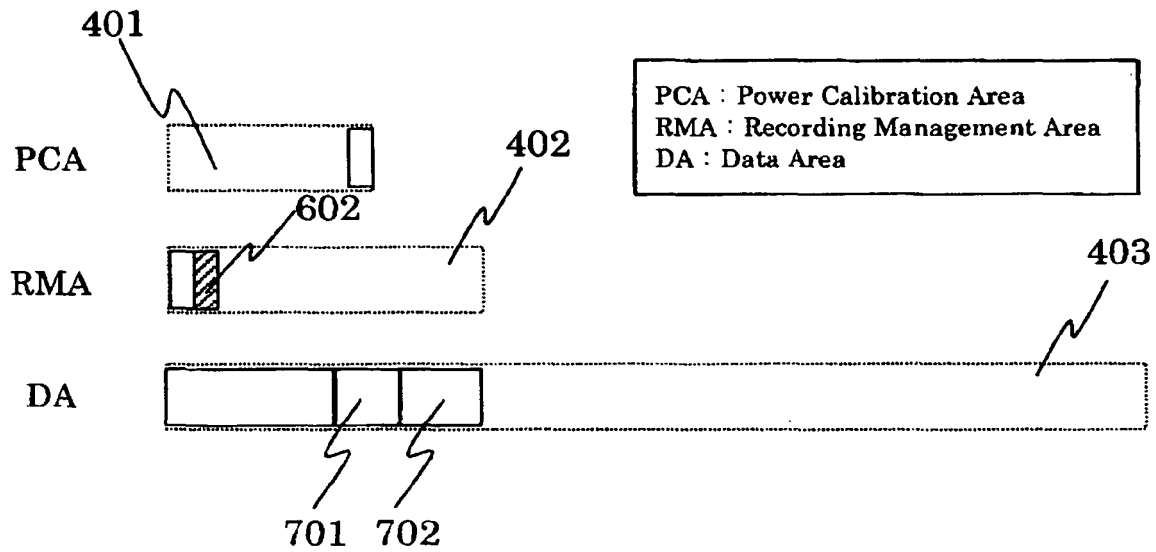
【図 6】

図 6



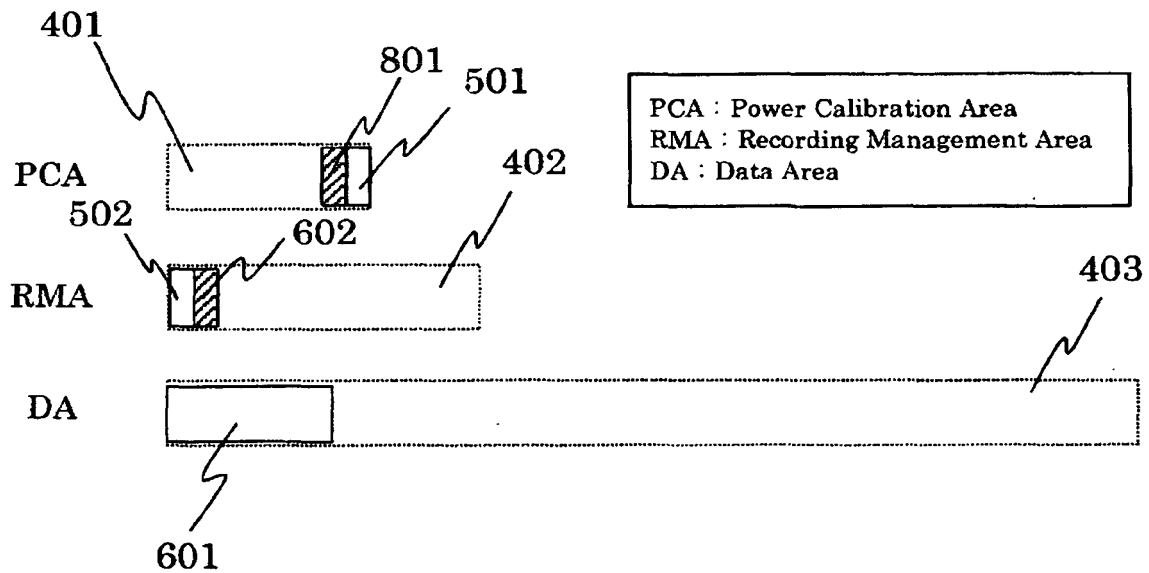
【図 7】

図 7



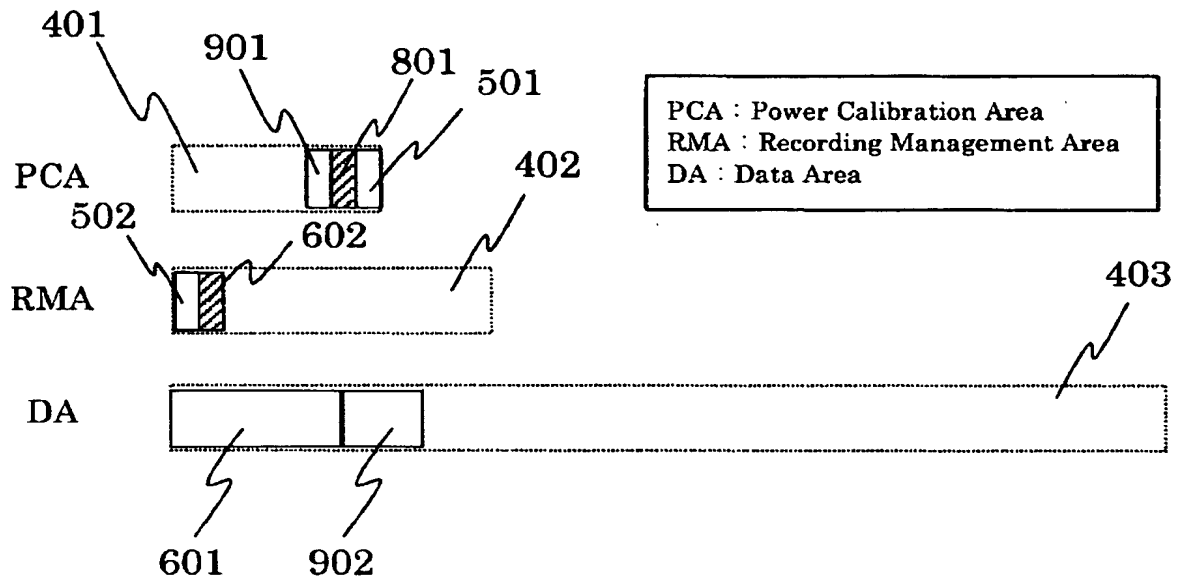
【図 8】

図 8



【図 9】

図 9



【書類名】 要約書

【要約】

【課題】

ディスク装置の起動処理の一環として行われる管理情報の確認処理を、データ領域の走査を行うことなく短時間で終了させることによって起動処理時間の短縮を図り、その結果としてディスク装置の応答性を高める。また、管理情報の確認処理に時間を要する場合に、その旨をディスク装置のホスト装置あるいはユーザーに知らしめるための機会をディスク装置に与え、ディスク装置がホスト装置あるいはユーザーに通報を行った上で管理情報の確認処理を行うことができるようにし、その結果としてディスク装置の応答性を高める。

【解決手段】

ディスクに記録された管理情報が有効であることを証明する認証情報と、この認証情報を無効化する認証無効化情報とを提供し、認証情報を無効化する認証無効化情報が存在する場合は管理情報が無効あるいは無効の可能性があると判定することを可能にし、また、認証情報を無効化する認証無効化情報が存在しない場合は、認証情報によって管理情報が有効であると判定することを可能にする。

【選択図】 図1

認 定 ・ 付 加 情 報

特許出願の番号	特願 2 0 0 3 - 0 7 6 7 8 8	
受付番号	5 0 3 0 0 4 5 4 6 0 7	
書類名	特許願	
担当官	第八担当上席	0 0 9 7
作成日	平成 1 5 年	3 月 2 4 日

・ < 認定情報・付加情報 >

・ 【提出日】 平成15年 3月20日

出 願 人 履 歴 情 報

識別番号 { 0 0 0 0 0 5 1 0 8 }

1. 変更年月日 1 9 9 0 年 8 月 3 1 日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台 4 丁目 6 番地

氏 名 株式会社日立製作所